ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 65, No. 12, pp. 2232~2239, 2016
http://dx.doi.org/10.5370/KIEE.2016.65.12.2232

모바일 메신저를 이용한 스마트 IoT 하드웨어 제어 시스템

Smart IoT Hardware Control System using Secure Mobile Messenger

이 상 형* · 김 동 현** · 이 해 연†
(Sang-Hyeong Lee · Dong-Hyun Kim · Hae-Yeoun Lee)

Abstract - IoT industry has been highlighted in the domestic and foreign country. Since most IoT systems operate separate servers in Internet to control IoT hardwares, there exists the possibility of security problems. Also, IoT systems in markets use their own hardware controllers and devices. As a result, there are many limitations in adding new sensors or devices and using applications to access hardware controllers. To solve these problems, we have developed a novel IoT hardware control system based on a mobile messenger. For the security, we have adopted a secure mobile messenger, Telegram, which has its own security protection. Also, it can improve the easy of the usage without any installation of specific applications. For the enhancement of the system accessibility, the proposed IoT system supports various network protocols. As a result, there are many possibility to include various functions in the system. Finally, our IoT system can analyze the collected information from sensors to provide useful information to the users. Through the experiment, we show that the proposed IoT system can perform well

Key Words : Internet of Things, Smart Home, Mobile Messenger, Naive Beyes, Bayesian Network

1. Introduction

With the wide use of mobile devices, the number of mobile applications and hardware devices are drastically increased. Also, the interest about Internet of Things (IoT) is increased with the use of IoT devices. In global business markets, IoT industries are rapidly growing and IoT devices are used in various areas. A smart home system is a representative application of the IoT system.

Since there are no standard platform of IoT systems in commercial markets and researches, each IoT systems and devices use their own platform and applications. In Korea, IoT systems in commercial markets use a separate server, which is usually operated by the IoT system provider. It means that all private information of the IoT system users are kept in this server. If this server is hacked, all private information of the users can be leaked. Moreover, the IoT devices and sensors of the smart IoT home system users can be controlled to harm.

Figure 1 shows the weakness of previous IoT system against attacks. When the system is hacked, there will be a great financial loss. Also, the fatal accident such as the fire of home can happen and the privacy can be revealed by monitoring the camera devices.

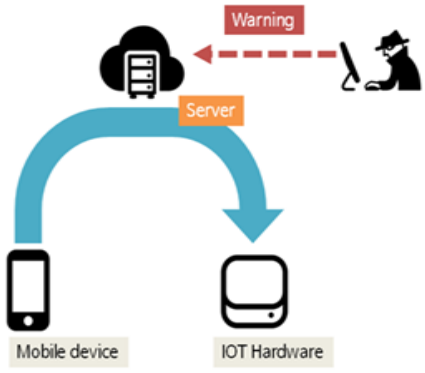

Fig. 1 Weakness against hacking of previous IoT

In order to resist against these hacking threats, the security policy of the server is required and the continuous security update is required for the IoT system providers. As a result, the cost of the IoT systems can be increased and that will disturb the wide usage of the IoT systems. Therefore, It performs communication between the user and IoT hardware by using a guaranteed security messenger program. There is no need for a central management server and the cost of building the system is low.

This paper proposes a novel IoT hardware control system

† Corresponding Author : Dept. of Software Engineering, Kumoh National Institute of Technology, Korea
E-mail: riscape@nate.com
Received : October 20, 2016; Accepted : November 2, 2016

against these security threats. For the security, we have adopted a secure mobile messenger, Telegram, which has its own security protection. Figure 2 shows the overall structure of the proposed system. Since the security of the mobile messenger is continuously updated, IoT system providers do not have to concern the security problems and invest the resource for the security. Moreover, it can improve the easy of the usage without any installation of specific applications.

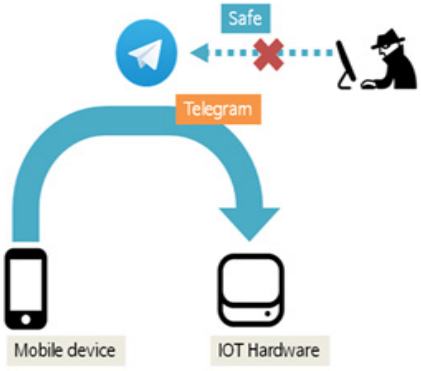

Fig. 2 Security enhancement of our IoT system.

To communicate IoT systems with devices or sensors, most commercial IoT systems can use their own products or products supporting protocols which are provided by communication service providers. As a results, there are many limitations in adding new devices or sensors. Also, the application software should be installed to control these new ones. Therefore, many IoT system providers are studying to preoccupy the IoT standard platform.

Our proposed IoT hardware control system supports various network protocols such as Zigbee, Bluetooth, WIFI, IR to connect pre-developed and newly developed devices and sensors. Therefore, all devices and sensors can be controlled and monitored using the mobile messenger.

Application software of IoT systems are used to control connected devices and monitor sensors. Most IoT systems in the market can only control devices and acquire the current information from sensors. Usually, IoT system providers are focused on the development of the platform.

The research to get the useful information from the collected information with big data processing or deep learning is a beginning stage. Since the IoT hardware control system can collect various information from devices and sensors, the useful information can be inferred with applying big data and deep learning methods. Although it is a beginning stage, the proposed IoT hardware system can collect various information from devices and sensors. And then it provides the useful information to the users by analyzing the collected information. The experiment shows the implementation of the proposed IoT hardware system and the test results show that the proposed IoT system can perform well.

The paper is organized as follows. Section 2 presents related works about smart IoT products and researches. In Section 3, our IoT hardware control system with a mobile messenger is proposed, in which security enhancement is addressed. Also, the way to increase the variety with supporting various protocols and the way to provide the useful information for the users are explained. Section 4 shows the implemented hardware system and its function. Also, experimental results from data analysis are presented. Section 5 concludes the paper.

2. Related Works

In Korea, many national projects related to IoT have been invested with the related developments of RFID/USN and M2M etc. IoT system companies, communication service providers and research institutes are co-operating to develop the common IoT platform for ensuring the IoT compatibility in automobile, medical treatment, home electricity, and power fields [1].

A company, Kyung-Dong Navien, has released an IoT home automation system to control heating. By installing an application, all function of boiler system can be controlled for heating. Also, remote control is possible by connecting lights and gas circuit breakers at home. An artificial intelligence system is introduced for the improvement to decide the appropriate quantity of heat for each room.

The smart home service is recently released by SKT, which can be used without any limitations of communication service providers or product developers. An IoT service can be provided by installing a bridge in the home and connecting devices with this bridge. For the convenience of the users, the bridge can be connected with door lock, dehumidifier, boiler, refrigerator, air-conditioner. Also, the usage of electricity can be provided to the user. Merely, each applications for each devices should be installed in the mobile device.

In KT, M2M and IoT platforms focusing on scalability, flexibility, massive data, cloud, and standardization have been studied. This platform has many application in various industry fields, which can support service and business process, minimize the cost of server installation with cloud services and provide the ability of big data processing with

massive collected data [2].

LG U Plus has studied the development of a M2M platform. This platform can guarantee the reliability of data from each device, make it easy to communicate with other systems and access devices by the users. Also, it supports many protocols to transfer data in various situations. However, since they connect the external IoT platform with IoT devices and sensors, only the network protocol supported by the external IoT platform is used [3].

Kelly et al. have studied an IoT system which is a low cost ubiquitous sensor system. It collects and monitors the environmental condition of home in periodic. After installing sensors in home, it collects environmental condition of home from sensors and decide the status of home [4].

Pang has studied the in-home health care devices and services. Using sensors attached to the user, the status of the user is checked and remotely sent to the doctor. [5].

Gomez et al. have designed the architecture to install network at home. Also, they have studied the network protocol for connecting each device based on wireless home network techniques such as Zigbee, Z-wave, INSTEON, wavenis, and IP-based technology [6].

Jie et al. have studied a smart home system based on IoT [7]. Baoan and Yu have researched about the implementation and management of an IoT system using detecting sensors such as IoT RFID, IR sensors, GPS etc. Also, they have designed an integrated interface to manage IoT devices communicating with RFID [8].

Wang et al. have developed a smart home system. Since many electric devices for home have been released, the management of these devices becomes an issue to make home as secure and safe places. Therefore, they have presented a management method of various systems and IoT devices using 433 MHz wireless sensors and WSAN [9].

Yang and Cho have studied a module-based Bayesian network for situation recognition at smart TV. Using smart TV applications and environmental information, domain-knowledge-based Bayesian networks are designed and the user situation is inferenced [10].

3. Smart IoT Hardware Control System with Mobile Messenger

In this section, the novel IoT hardware control system is proposed. The overall structure of our IoT hardware control system with a mobile messenger are depicted in Figure 3.

Because there is no central server, server installation cost is not consumed. The costs of the IoT devices and IoT gateways installed in the house are the same. However, the user communicates with the IoT Gateway using telegrams that are freely available on mobile devices. Therefore, the server construction cost and the communication cost through the server are reduced.

At home, smart IoT gateway is connected with various IoT sensors and devices. This gateway collects data from these connected devices and sensors. Mobile devices access the smart IoT gateway to get the home situation. For the communication between mobile devices and the smart IoT gateway, mobile messenger is adopted for the security enhancement, the support of various network protocols and the compatibility with other IoT products.

After the user is authenticated for the smart IoT gateway to securely control IoT devices at home, this gateway receive a message from the mobile messenger to perform. Also, this gateway sends home situation information to connected users based on the analysis of user pattern. This gateway can receive external data to store and use.

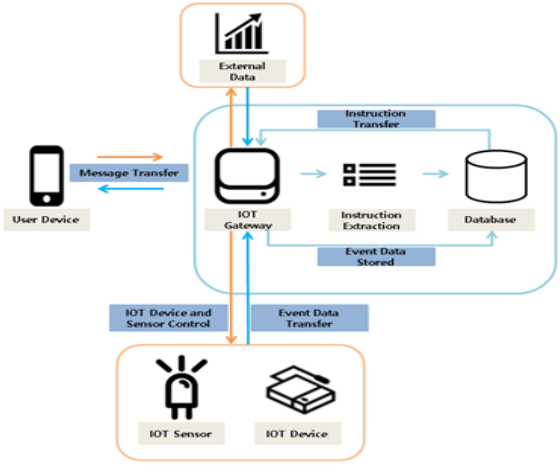

Fig. 3 Smart IoT Home System Structure and its Working Procedure

As depicted in Figure 3, the procedure for the user to control IoT devices and sensors or receive information from the IoT gateway is as follows. (1) The user sends a message using mobile device to the IoT gateway. (2) When the IoT gateway receives the message, it recognizes the specific command in the user message using database, in which commands are classified. (3) After command recognition, the IoT gateway sends control signals to IoT devices and sensors. (4) When events happen in IoT devices and sensors, the IoT gateway saves the data in database. (5) Also, with these events, the IoT gateway sends command execution results from IoT devices and sensors to the user.

3.1 Security Enhancement using Mobile Messenger

As explained before, most IoT systems and devices in markets use a specific server to send and receive commands and data. When this server is hacked, users will lost the control of IoT systems and devices. Also, since this server has important data including private information, there will be a fatal accident such as financial loss or fire. To solve these problems, our IoT hardware control system has adopted a secure mobile messenger such as Telegram for communication between users and the IoT gateway.

When the users install a secure mobile messenger in mobile devices, they can communicate with the IoT gateway in the home. Control commands of the users are sent by typing the message using the mobile messenger. Also, the information from the IoT gateway are sent to the user by receiving the message using the mobile messenger. The IoT gateway saves all collected information from IoT devices and sensors and these information can be only accessed through the mobile messenger.

In our system, the authenticated users in the mobile messenger can send commands to the IoT gateway. Therefore, although the mobile messenger is attacked, the user authentication information is stored in the mobile device and hence the control ability of the IoT gateway can be protected. Although the message of mobile devices is hacked by novice, it is a commonly used text message and novice cannot notice it as an IoT gateway control commands. Moreover, the cost to protect and update the server against attacks can be saved, which is critical for small IoT companies.

In case of most IoT platforms in markets, mobile applications on the mobile device are used to control IoT devices and sensors at home. In this case, application should be installed and updated in the mobile device of the users. Sometimes, the users should install many applications to control each IoT device and sensor. However, in our IoT hardware control system, the IoT gateway communicates with the users using the mobile messenger. After receiving the message from the users, the IoT gateway recognize the command and then control the IoT devices and sensors as depicted in Figure 4. Therefore, to control IoT devices and sensors, the users can only install a mobile messenger without installing specific applications.

3.2 Various Network Protocol Supports

Most IoT systems and devices on sales operate in wireless network environments such as Bluetooth or WIFI. These systems and devices support various network protocols and have different setting methods depending on providers. Therefore, IoT devices and sensors from different providers have a difficulty in their integration. In our IoT hardware control system, the IoT gateway is designed to support various network protocols as shown in Figure 5. As a result, our system can be easily expanded and add new IoT devices and sensors from most providers.

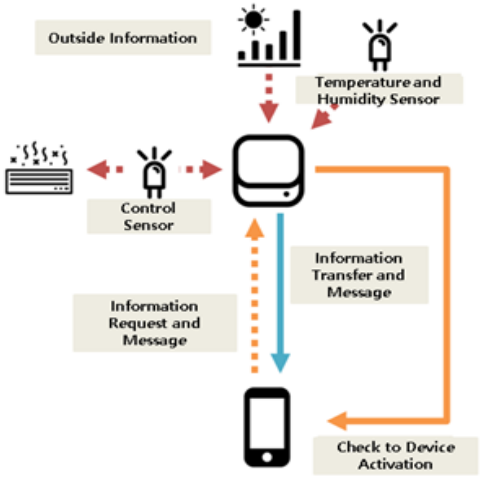

Fig. 4 Intercation between Users and the IoT Gateway

Fig. 5 Supporting Various Network Protocols in out IoT Gateway

3.3 Collected Information Analysis

In the smart IoT home system, the IoT gateway is connected with various IoT devices and sensors and hence it can collect data from devices and sensors. Most IoT companies for the smart IoT home focus on the development of the standard platform. The research using collected information with big data or deep learning is a beginning stage.

This section explains the preliminary study about using collected information with big data processing methods. In our IoT hardware control system, the IoT gateway collects

data from temperature and humidity sensors that are installed at home. Then, an algorithm in the IoT gateway is trained with temperature and humidity which is comfortable for users and inference the status of home. This algorithm is designed based on naïve bayes theorem as equations (1) and (2).

$$posterior(A) = \frac{p(A) \times p(a|A) \times p(b|A)}{evidence} \quad (1)$$

$$posterior(B) = \frac{p(B) \times p(a|B) \times p(b|B)}{evidence} \quad (2)$$

The posterior(A) is the posterior probability when the status of home is comfortable. The posterior(B) is the posterior probability when the status of home is uncomfortable. is the probability of the comfortable status among all training data and is the probability of a uncomfortable status among all training data. Variable is the temperature value of the status to be determined. is the conditional probability of the comfortable temperature status. The evidence is a normalized constant from an equation (3).

$$evidence = p(A)p(a|A)p(b|A) + p(B)p(a|B)p(b|B) \quad (3)$$

By comparing these calculated posterior(A) and posterior (B), the current status is determined. These inference results are saved in the database of the IoT gateway. The IoT gateway can provide this information to the user using the mobile messenger. Also, the IoT gateway can control the temperature and the humidity of home to be a comfortable status for the users.

Adding various IoT devices and sensors can increase the uncertainty of the home status. In order to inference in uncertain status, we have designed a Bayesian network which is a kind of directed a cyclic graph. Using the calculated posterior probability from the above Bayes theorem, the Bayesian network is set with the status category probability model. This probability model is the equation (4).

$$p(H_i|E) = \frac{p(E|H_i)p(H_i)}{\sum_{k=1}^{n} p(E|H_k)p(H_k)}, i = 1,2,3 \cdots n \quad (4)$$

Using this formula for the probability model, the Bayesian network model can be designed as depicted in Figure 6.

The status category probability model is composed of 3 layers: input layer, relation layer, and target layer. The input layer has input nodes which have a prior probability to inference relation and target nodes. The relation layer has relation nodes which have a highest association with target nodes. The target layer has target nodes which represent the status to be inferred from input and relation node values. To apply for the designed Bayesian network model and inference the home status, the information from our smart IoT home system is classified as shown in Table 1.

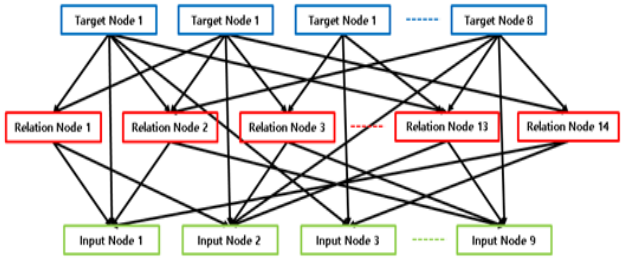

Fig. 6 Designed Bayesian Network Model

Table 1 Data Classification Table from Smart IoT Home

Classification	Data
Time	0 ~ 24
State	Sleep, Inside Activation, Outside Activation
Temperature Sensor	High, Medium, Low
Humidity Sensor	High, Medium, Low
Illumination Sensor	High, Medium, Low
Dust Sensor	High, Medium, Low
Boiler Control Sensor	On, Off
Air Conditioner Control Sensor	On, Off
TV Control Sensor	On, Off

Table 2 Situation Category Design at Bayesian Network

Node	Category
Input Node	Time, State, Temperature, Humidity, Illumination, Dust, Boiler, Air Conditioner, TV
Relation Node	Sleep, Inside Activation, Outside Activation, Using Boiler, Using Air Conditioner, Using TV
Target Node	Situation

Using the classified smart IoT home information, the nodes of the Bayesian network are set and connected. Table 2 summarizes the status category classification for the Bayesian network.

4. Experiments Result

We have implemented the proposed smart IoT hardware

control system including the smart IoT gateway connected with IoT devices and sensors and communicating with Telegram. Telegram whose high security is well known in markets is used for communication between the user and the IoT gateway. The user can transfer a command to the IoT gateway by typing a text message through Telegram. The IoT gateway can control IoT devices and sensors by analyzing the text message from Telegram and send an information to the user.

Figure 7 shows the smart IoT gateway developed with Arduino and Raspberry Pi. The smart IoT gateway includes Bluetooth, Zigbee, WIFI and IR modules to communicate with IoT devices and sensors. This IoT gateway is connected on Internet, but IoT devices and sensors are not connected on Internet.

Fig. 7 Picture of Smart IoT Gateway

Table 3 summarizes IoT devices and sensors connected to the smart IoT gateway using various network protocols such as Bluetooth, WIFI and IR.

Table 3 Connected IoT Devices and Sensor

Classification	Name	Network Protocol
Hue	Table	WiFi
Hue	Hue24	WiFi
Light	Light	Bluetooth
Multi Tap	Multi Tap	WiFi
Sensor	Window	WiFi
Sensor	Gas	WiFi
Sensor	Door	Bluetooth
Sensor	Remote Control	IR
Sensor	Desk	WiFi

Each IoT devices and sensors send an information to the smart IoT gateway when an event happens. Also, when the user transfers a command to activate these devices and sensors, the information is sent to the smart IoT gateway. The smart IoT gateway collects the received information into the database. Figure 8 shows a database modeling to store the information.

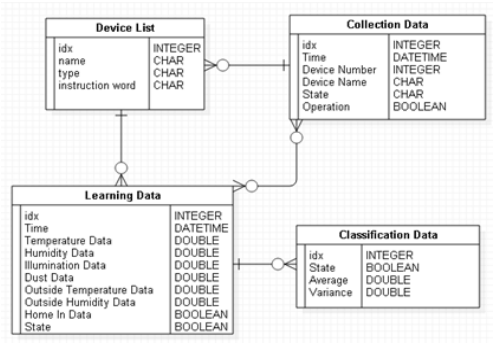

Fig. 8 Database Modeling for Storing Smart IoT Home Information

The smart IoT gateway can inference the status of the home using the stored information. The time of the event, the status of the devices, and the working status are used for the home status inference.

For the experiment, the Bayesian network model is trained by configuring the experimental condition. When current measured values '14 hour, internal action, temperature medium, humidity medium, illumination Low, boiler off, air conditioner off, TV on' are entered in the trained Bayesian network model, the inference result is shown in Table 4.

Table 4 Inferred Smart Home Status using Bayesian Network Model

Target Situation	Inference Probability
Comfortable status at sleeping	0%
Uncomfortable status at sleeping	0%
Comfortable status at watching TV	53%
Uncomfortable status at watching TV	4%
Comfortable status at internal activity	39%
Uncomfortable status at internal activity	4%

Based on the result, the probability of the status 'comfortable status at watching TV' is 53% and the probability of the status 'comfortable status at internal activity' is 39%. By comparing two results, we can determine the current status as 'comfortable status at watching TV'. The IoT gateway sends this inference result to the user via Telegram. Then, the users can control IoT

devices and sensors depending on their preference via Telegram.

Figure 9 shows the captured images of Telegram on the mobile device at the user side. The user can send a message to the smart IoT gateway and receive the information from the IoT gateway using Telegram.

Fig. 9 Captured Image of Telegram on the Mobile Device

When a command "weather" is sent to the smart IoT gateway, it immediately return a result of current local weather. When the command is "door lock", the door lock status attached in the entrance door is returned. When the command is "temperature", the in-door temperature of home is returned. In order to control IoT devices and sensors connected to the smart IoT gateway, the user can send a command "on" and "off" with the name of IoT devices or sensors. When the IoT gateway receives the command, it recognizes and execute the command to control IoT devices and sensors. Also, the execution results are returned to the user.

5. Conclusion

In domestic and foreign countries, IoT industry has been highlighted and the smart IoT home systems are starting sales on markets. In this paper, we proposed a novel smart IoT hardware control system using a secure mobile messenger. The proposed system can provide the easy to use and manage for the users and increase the security against attacks.

Differently from smart IoT home systems in markets using the specific server, the proposed system is secure with the use of a secure mobile messenger for communication. Since the mobile messenger can support the end-to-end encryption, the smart IoT hardware control system can be protected against hacking and malicious attempts. Moreover, the use of a mobile messenger can avoid the installation of various application software for each IoT devices and hence increase the efficiency of the management and integration of IoT devices and sensors. Since the IoT gateway supports various network protocols such as Bluetooth, WIFI, Zigbee, and IR, the proposed IoT hardware control system can achieve the scalability and generality, in which new IoT devices and sensors can be easily added by users. The IoT gateway can collect information from IoT devices and sensors and these information can be analyzed using a big data processing model to inference the status of the home and sent to the users using the mobile messenger. When IoT devices and sensors are added more, the correct and various inference information can be sent to the users.

The proposed system using the secure mobile messenger is very efficient in cost against most IoT systems in markets, which use a specific server for communication and require specific applications or sometimes many applications for each device and sensors.

The cost of installing the system inside the house is low. In addition, communication cost can be efficiently used because the user communicates directly with the IoT gateway using the mobile device without going through the central server, communication costs can also be used efficiently. It can control the IoT device by analyzing the status of the inside of the house, communicating the information, and analyzing the status of the user. The convenience of the user is increased because various information is transmitted and the devices are controlled according to the state of the user.

With the highlighting of IoT markets, various IoT devices and sensors are emerging and the implementation of the IoT platform and the security will be issues. As future works, the integrity platform for the user convenience should be studied. Also, the enhancement of the security against hacking and malicious attacks should be continuously studied.

Acknowledgements

This work was supported by the research fund of National Security Research Institute (2016-082) and the business fund (Grants No. 1425095296) for Cooperative R&D between Industry, Academy, and Research Institute by Korea Small and Medium Business Administration in 2015.

References

[1] S. C. Choi, M. W. Ryu, N. Jin, and J. H. Kim, "IoT Platform and Service Trends," Journal of the Korean Institute of Communication Sciences, Vol. 31, No. 6, pp. 20-27, 2014.

[2] W. B. Jeon and S. H. Baek, "M2M/IoT Service Platform of KT," Journal of Korean Institute of Communication and Information Sciences, Vol. 30, No. 8, pp. 40-45, 2013.

[3] H. S. Yang, "M2M/IoT Platform and Service of LG U+," Journal of the Korean Institute of Communication Sciences, Vol. 30, No. 8, pp. 46-52, 2013.

[4] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the implementation of IoT for environmental condition monitoring in homes," IEEE Sensors Journal, Vol. 13, No. 10, pp. 3846-3853, 2013.

[5] Z. Pang, "Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being," Doctoral Thesis, KTH Royal Institute of Technology, 2013.

[6] C. Gomez, and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," IEEE Communications Magazine, Vol. 48, No. 6, pp. 92-101, 2010.

[7] Y. Jie, J. Y. Pei, L. Jun, G. Yun, and X. Wei, "Smart home system based on IOT technologies," Proceeding of the International Conference on Computational and Information Sciences (ICCIS 2013), pp. 1789-1791, 2013.

[8] B. Li, and J. Yu, "Research and application on the smart home based on component technologies and Internet of Things," Procedia Engineering, Vol. 15, pp. 2087-2092, 2011.

[9] M. Wang, G. Zhang, C. Zhang, J. Zhang, and C. Li, "An IoT-based appliance control system for smart homes," Proceedings of the International Conference on Intelligent Control and Information Processing (ICICIP 2013), pp. 744-747, 2013.

[10] K.-M. Yang, and S.-B. Cho, "Modular Bayesian Networks for Context-Awareness in Smart TV," Journal of KISS: Software and Applications, Vol. 40, No. 2, pp. 108-121, 2013.

저 자 소 개

Sang-Hyeong Lee

received his Bachelor of Engineering in computer software engineering from Kumoh National Institute of Technology in 2015. He is now with the master's course. His major interests are image processing, machine learning.

Dong-Hyun Kim

received his Bachelor of Engineering in computer software engineering from Kumoh National Institute of Technology in 2016. He is now with the master's course. His major interests are image processing, machine learning.

Hae-Yeoun Lee

received his MS and PhD degrees in computer science from Korea Advanced Institute of Science and Technology (KAIST) in 1997 and 2006, respectively. From 2001 to 2006, he was with Satrec Initiative, Korea. From 2006 to 2007, he was a postdoctoral researcher at Weill Medical College, Cornell University, United States. He is now with Kumoh National Institute of Technology, Korea. His major interests are image processing, digital watermarking, digital forensics, remote sensing, and digital rights management.